代数学 I 第 3 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

前回，群と部分群の抽象的な定義について学び，その中で $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ や $(\mathbb{Q}^\times,\times)$, $(\mathbb{R}^\times,\times)$, $(\mathbb{C}^\times,\times)$ といった慣れ親しんだ数の体系が群の例を与えることを見た．今回は新たな数の体系として整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$ と呼ばれるものを導入し，ここでの演算によって再び群の例が与えられることを見る[*1]．また，この数の体系を扱うにあたっては well-defined 性という考え方を習得することが重要である．well-defined 性は代数学 I の講義を通して非常に重要であるが，慣れるまでとっつきにくいものかもしれないので，ここの例で良く理解しておいてほしい．

2.1 整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$

定義 2.1

$n\in\mathbb{Z}_{>0}$ とする．各 $a\in\mathbb{Z}$ に対し，$[a]_n$ という記号を割り当てる．ただし，$a,b\in\mathbb{Z}$ に対し，$[a]_n$ と $[b]_n$ を次のルールで同一視する：

$$\begin{aligned}[a]_n=[b]_n &\Leftrightarrow a-b \text{ が } n \text{ で割り切れる } (\Leftrightarrow a\equiv b \mod n)\\ &\Leftrightarrow \text{ある } k\in\mathbb{Z} \text{ が存在して，} a=b+kn.\end{aligned}\tag{2.1}$$

このとき，

$$\mathbb{Z}/n\mathbb{Z}\coloneqq\{[a]_n\mid a\in\mathbb{Z}\}=\{[0]_n,[1]_n,\dots,[n-1]_n\}\tag{2.2}$$

とする．これを n **を法とする整数の剰余類環 (the ring of integers modulo** n**)** という．ここで，同一視のルールにより，$[a]_n=[b]_n$ となる必要十分条件は a と b を n で割った余りが等しいことであり，整数を n で割った余りは $0,1,\dots,n-1$ のいずれかであることから，(2.2) の 2 つめの等号は示される．

なお，「$\mathbb{Z}/n\mathbb{Z}$」という記号については $\mathbb{Z}$, $/$, $n\mathbb{Z}$ というように分解して意味を考えるのではなくて，「$\mathbb{Z}/n\mathbb{Z}$」で 1 つの記号として考えてほしい．この記号の “意味” は先の講義でわかることになる．

例 1. 同一視 (2.1) の例は以下のようなものである．

- $\mathbb{Z}/5\mathbb{Z}$ において，$[2]_5=[7]_5=[-3]_5=\cdots$
- $\mathbb{Z}/360\mathbb{Z}$ において，$[90]_{360}=[-270]_{360}=[450]_{360}=\cdots$

この計算は角度計算のように考えればこれまで十分慣れ親しんだものと言えるだろう ($90^\circ=-270^\circ=450^\circ$)．

$\mathbb{Z}/n\mathbb{Z}$ は n 個の元からなる有限集合であるが，ここに以下の方法で二項演算を定義する：

$$\begin{aligned}+&\colon \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z},\ ([a]_n,[b]_n)\mapsto[a+b]_n\\ -&\colon \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z},\ ([a]_n,[b]_n)\mapsto[a-b]_n\\ \times&\colon \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z},\ ([a]_n,[b]_n)\mapsto[ab]_n.\end{aligned}$$

* *e-mail* : hoya@shibaura-it.ac.jp

*1 整数の剰余類環はその名の通り，数学においては**環**と呼ばれる対象として扱われるのが通常である．環とは簡単に言えば「加法と乗法が定まっているような数の体系」である．厳密な定義については代数学の基本的な参考書を参照すること．

例 2.

$$[2]_7+[5]_7=[7]_7=[0]_7 \qquad [2]_7-[5]_7=[-3]_7=[4]_7 \qquad [2]_5\times[3]_5=[6]_5=[1]_5.$$

ここで重要なのがこれらの二項演算が “ちゃんと定義されている” かどうか (**well-defined 性**) の確認である.

重要 (well-defined 性について)

(2.1) において a,b を有理数と考えて，$[a]_n$ の定義を $a\in\mathbb{Q}$ に拡張してみよう[*2]．例えば，

$$[0.5]_2=[2.5]_2=[-1.5]_2$$

等である．正の整数 $n\in\mathbb{Z}$ に対して，$\mathbb{Q}/n\mathbb{Z}=\{[r]_n\mid r\in\mathbb{Q}\}$ とする．このとき，

$$\times\colon \mathbb{Q}/n\mathbb{Z}\times\mathbb{Q}/n\mathbb{Z}\to\mathbb{Q}/n\mathbb{Z},\ ([r]_n,[s]_n)\mapsto[rs]_n.$$

は定義されるだろうか? 実は以下のような困ったことが起こってしまう：

$$\begin{array}{ccc}[1.5]_2\times[2]_2=[1.5\times2]_2=[3]_2\\ \| \qquad\qquad \not= \\ [1.5]_2\times[0]_2=[1.5\times0]_2=[0]_2.\end{array}$$

よって，この写像の定義は実は良くない (きちんと定義されていない) ということがわかる．なぜこのようなことが起こるかというと，『$\mathbb{Q}/n\mathbb{Z}$ の中では，1 つの元を表す方法が何通りもある ($[2]_2=[0]_2$ 等) にもかかわらず，写像の定義において特定の表示 ($[r]_n$ や $[s]_n$ の r や s のこと) を用いてしまった』からである．この結果，同じ元なのに，表し方が違ったがために結果が変わるということになってしまったのである．

このように，**1 つの元の表し方が複数あるような集合からの写像を定義する際には細心の注意を払う必要がある**．定義した写像が元の表示の仕方に依らないとき，その写像は **well-defined** であるという．well-defined 性の注意は慣れるまで難しいと思われるが，今後の講義でも非常に重要になる．

上で定義した $\mathbb{Z}/n\mathbb{Z}$ における $+,-,\times$ は実は全て well-defined である．試しに $\times\colon\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ が well-defined であることを示そう．写像の定義域から選んで来た元について，どのような表示をとっても写像で送った結果が変わらないということを言えばよい.

証明. $[a]_n=[a']_n$, $[b]_n=[b']_n$ $(a,a',b,b'\in\mathbb{Z})$ であると仮定する．このとき，(2.1) から，ある $k_1,k_2\in\mathbb{Z}$ が存在して，

$$a'=a+k_1n \qquad b'=b+k_2n$$

と書ける．これより，

$$\begin{aligned}[a']_n\times[b']_n&=[(a+k_1n)(b+k_2n)]_n\\&=[ab+(ak_2+bk_1+k_1k_2n)n]_n\end{aligned}$$

となるが，いま$ak_2+bk_1+k_1k_2n$ は整数なので，結局 $[a']_n\times[b']_n=[ab]_n=[a]_n\times[b]_n$ となる．これより，well-defined であることが示された． □

a,b が有理数の場合には下線部分が言えないので，well-defined ではなかったのである．この調子で，$\mathbb{Z}/n\mathbb{Z}$ 上の二項演算 $+,-$ が well-defined であることを確認してもらいたい．ちなみに，$+$ や $-$ に関しては $\mathbb{Q}/n\mathbb{Z}$ においても well-defined に拡張される.

well-defined 性について慣れるために，well-defined である写像とそうでない写像の例をもう少し出しておこう.

[*2] ちゃんと言うと，「$a-b$ が n で割り切れる」は「$a-b$ が n で割り切れる整数である」に修正する.

例 3. 写像

$$f_1 \colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z},\ [a]_6 \mapsto [a]_3$$

は well-defined である．なぜなら，$[a]_6 = [a']_6$ $(a, a' \in \mathbb{Z})$ であるとき，(2.1) からある $k \in \mathbb{Z}$ が存在して，$a' = a + 6k$ と書け，このとき，

$$f_1([a']_6) = [a']_3 = [a + 6k]_3 = [a + 3 \cdot 2k]_3 = [a]_3 = f_1([a]_6)$$

となるためである．

一方，写像

$$f_2 \colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z},\ [a]_5 \mapsto [a]_3$$

は well-defined ではない．なぜなら，$[0]_5 = [5]_5$ であるにもかかわらず，

$$f_2([0]_5) = [0]_3 \neq [2]_3 = [5]_3 = f_2([5]_5)$$

となるためである．

2.2 $\mathbb{Z}/n\mathbb{Z}$ の群構造

話を $\mathbb{Z}/n\mathbb{Z}$ での二項演算に戻そう．正の整数 $n \in \mathbb{Z}_{>0}$ に対して，$(\mathbb{Z}/n\mathbb{Z}, +)$ は群である．これを n を法とする**整数の剰余類群**という．$\mathbb{Z}/n\mathbb{Z}$ の $+$ は $\mathbb{Z}$ の通常の加法 $+$ に由来しているので群の二項演算の 3 性質が成立することはほぼ明らかではあるが，一応確認してみよう．

(I) (結合法則) 任意の $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，

$$([a]_n + [b]_n) + [c]_n = [a + b + c]_n = [a]_n + ([b]_n + [c]_n).$$

(II) (単位元の存在) 単位元は $[0]_n \in \mathbb{Z}/n\mathbb{Z}$ である．実際，任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，

$$[0]_n + [a]_n = [a]_n = [a]_n + [0]_n$$

が成立する．

(III) (逆元の存在) 任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[-a]_n \in \mathbb{Z}/n\mathbb{Z}$ であって，

$$[-a]_n + [a]_n = [0]_n = [a]_n + [-a]_n$$

が成立する．($[a]_n$ の逆元 $[-a]_n$ は $[a]_n^{-1}$ ではなく $-[a]_n$ としばしば書かれる．)

さらに，$+$ は

(IV) 任意の $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[a]_n + [b]_n = [a + b]_n = [b]_n + [a]_n$

をみたすので，これは可換群である．また，$|\mathbb{Z}/n\mathbb{Z}| = n$ であったので，これは位数 n の有限群である．この例によって，全ての正の整数 $n \in \mathbb{Z}_{>0}$ に対し，位数 n の群が少なくとも 1 つ存在するということがわかったことになる．

次に $(\mathbb{Z}/n\mathbb{Z}, +)$ の部分群について考えてみよう．$(\mathbb{Z}/n\mathbb{Z}, +)$ の部分群は以下のように完全に記述できる．

定理 2.2

$n \in \mathbb{Z}_{>0}$ とする．k を n の約数としたとき，

$$H_k \coloneqq \{[ka]_n \mid a \in \mathbb{Z}\} \subset \mathbb{Z}/n\mathbb{Z}$$

は $(\mathbb{Z}/n\mathbb{Z}, +)$ の位数 n/k の部分群である．さらに，$(\mathbb{Z}/n\mathbb{Z}, +)$ の部分群はこの形のもので尽くされる．

証明. H_k が位数 n/k の部分群であること：任意の 2 元 $[ka]_n, [kb]_n \in H_k$ に対し，

$$[ka]_n + [kb]_n = [ka + kb]_n = [k(a + b)]_n \in H_k, \qquad -[ka]_n = [-ka]_n = [k(-a)]_n \in H_k$$

となるので，命題 1.5 より H_k は $\mathbb{Z}/n\mathbb{Z}$ の部分群である．さらに，$n = \ell k$ としたとき，$[\ell k]_n = [n]_n = [0]_n$ であることに注意すると，H_k は具体的には

$$H_k = \{[0]_n, [k]_n, [2k]_n, \ldots, [(\ell - 1)k]_n\}$$

と書ける．よって，H_k の元の個数は $\ell = n/k$ 個である．
部分群が H_k の形のものに限られること：まず自明な部分群については，

$$H_n = \{[0]_n\}, \quad H_1 = \mathbb{Z}/n\mathbb{Z}$$

となるので確かに H_k の形をしている (1 も n も n の約数であることに注意)．次に，$\mathbb{Z}/n\mathbb{Z}$ の非自明な部分群 H が必ず n のある約数 k を用いて H_k の形で書けることを示そう．$[k]_n \in H$ となる $1 \leq k \leq n - 1$ で最小のものを k_0 とする．(H は非自明なので $[0]_n$ 以外の元を少なくとも 1 つは含むため，このような k_0 は必ず 1 つ定まる．) まずこのとき，

$$H = H_{k_0} \coloneqq \{[k_0 a]_n \mid a \in \mathbb{Z}\}$$

であることを示す．H は部分群であるから，$[k_0]_n$ を何度も足し合わせたもの，およびその逆元を全て含むので，

$$H_{k_0} = \{[k_0 a]_n \mid a \in \mathbb{Z}\} \subset H$$

である．次に，$[m]_n \in H$ かつ $[m]_n \notin H_{k_0}$ となる $[m]_n$ $(1 \leq m \leq n - 1)$ が存在したとする．このとき，m を k_0 で割った商を q，余りを r とすると，$0 \leq r < k_0$ で，

$$m = k_0 q + r$$

である．いま，$[k_0 q]_n \in H_{k_0} \subset H$ であることに注意すると，H は部分群であることより，$[m]_n - [k_0 q]_n = [r]_n$ も H の元である．ここで，$r < k_0$ なので $r \geq 1$ だと，これは k_0 の最小性に反する．よって，$r = 0$，つまり，$m = k_0 q$ となる．しかし，このとき $[m]_n = [k_0 q]_n \in H_{k_0}$ となり，$[m]_n$ の取り方に矛盾する．よって，背理法により，このような $[m]_n$ は存在せず，$H = H_{k_0}$ であることがわかる．

最後に k_0 が n の約数であることを示そう．n を k_0 で割った商を q'，余りを r' とすると，$0 \leq r' < k_0$ で，

$$n = k_0 q' + r'$$

である．ここで，$[n]_n = [0]_n \in H_{k_0}, [k_0 q']_n \in H_{k_0}$ であることより，H_{k_0} が部分群であることに注意すると，$[n]_n - [k_0 q']_n = [r']_n$ も $H_{k_0} = H$ の元となる．ここで，$r' < k_0$ なので $r' \geq 1$ だと，これは再び k_0 の最小性に反する．よって，$r' = 0$，つまり，$n = k_0 q'$ となる．よって，k_0 は n の約数である． □

例 4. $(\mathbb{Z}/12\mathbb{Z}, +)$ の部分群は以下で全てである．

$$H_{12} = \{[0]_{12}\}, \quad H_6 = \{[0]_{12}, [6]_{12}\}, \quad H_4 = \{[0]_{12}, [4]_{12}, [8]_{12}\}, \quad H_3 = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\},$$
$$H_2 = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}, \quad H_1 = \mathbb{Z}/12\mathbb{Z}.$$

注意 1. 定理 2.2 の証明で，H_k が部分群であることを示す部分においては「k が n の約数である」という条件を用いていないことに注意する．実際，任意の $k \in \mathbb{Z}$ に対して，

$$H_k \coloneqq \{[ka]_n \mid a \in \mathbb{Z}\}$$

は $\mathbb{Z}/n\mathbb{Z}$ の部分群である．この定理が主張しているのは，「k が n の約数である」という条件を付ければ $\mathbb{Z}/n\mathbb{Z}$ **の部分群が過不足なく得られる**ということである (つまり，k が n の約数である場合を考えるだけで部分群は全て見つかり，しかも k と k' が n の異なる約数であるとき，$H_k \neq H_{k'}$)．例えば，$\mathbb{Z}/8\mathbb{Z}$ においては，

$$H_6 = \{[6a]_8 \mid a \in \mathbb{Z}\} = \{[-2a + 8a]_8 \mid a \in \mathbb{Z}\} = \{[-2a]_8 \mid a \in \mathbb{Z}\} = \{[2a]_8 \mid a \in \mathbb{Z}\} = H_2$$

となる．6 は 8 の約数ではないが，結局 H_6 は H_2 と一致するので，部分群を列挙するに当たっては考える必要はないのである．

k と k' が n の異なる約数であるとき，$H_k \neq H_{k'}$ となることは，位数が異なることから直ちにわかる．

2.3 復習：拡張ユークリッド互除法

次回 $\mathbb{Z}/n\mathbb{Z}$ における $\times$ を二項演算として実現される群を扱う．先に少し述べておくと，$(\mathbb{Z}\setminus\{0\},\times)$ が群にならなかった (第 1,2 回講義資料例 3) のと同様に $((\mathbb{Z}/n\mathbb{Z})\setminus\{[0]_n\},\times)$ も群になるとは限らない．一方で，$\mathbb{Z}\setminus\{0\}$ の部分集合で $\times$ に関して群をなすものは $\{1\}$ と $\{1,-1\}$ のみであったのに対し，$(\mathbb{Z}/n\mathbb{Z})\setminus\{[0]_n\}$ の場合は必ずしも $\{[1]_n\}$ と $\{[1]_n,[-1]_n\}$ のみではない．状況はもう少し複雑で，それを調べるためには，**拡張ユークリッド互除法**について思い出す必要がある．ここでは，次回の準備として，具体例をもとにその方法を思い出そう．厳密な原理については，補足プリント「拡張ユークリッド互除法について」を参考にすること．

定義 2.3

正の整数 a,b に対して，その最大公約数 (greatest common divisor) を $\gcd(a,b)$ と書く．さらに 0 以上の整数 a に対して，$\gcd(0,a)=\gcd(a,0)=a$ とする．

正の整数 a,b が与えられたときに，$\gcd(a,b)$ を効率良く求める方法がユークリッド互除法である．例として，2394 と 714 の最大公約数 $\gcd(2394,714)$ を求めてみよう．

ユークリッド互除法を用いて $\gcd(2394, 714)$ を求める

(Step 1) 大きい方の数を小さい方の数で割る：

$$2394 = \underset{\text{商}}{\underline{3}} \times 714 + \underset{\text{余り}}{\underline{252}}. \tag{2.3}$$

このとき，以下のようにして $\gcd(2394, 714) = \gcd(714, 252)$ であることがわかる．

$m = \gcd(2394, 714)$ とすると，714 と 2394 は共に m の倍数であるから，

$$[252]_m = [252 + 3 \times 714]_m = [2394]_m = [0]_m$$

なので，252 も m で割り切れる．よって，$\gcd(2394, 714) = m \leq \gcd(714, 252)$.

一方，$n = \gcd(714, 252)$ とすると，714 と 252 は共に n の倍数であるから，

$$[2394]_n = [3 \times 714 + 252]_n = [0]_n$$

なので，2394 も n で割り切れる．よって，$\gcd(714, 252) = n \leq \gcd(2394, 714)$.

以上より，$\gcd(2394, 714) = \gcd(714, 252)$.

一般の状況での厳密な証明は補足プリント「拡張ユークリッド互除法について」の命題を参照のこと．(証明方法はこの議論を一般的に書くだけである．)

(Step 2) 元の問題は $\gcd(714, 252)$ を求める問題に変わったので，714 と 252 に対して，(Step1) を繰り返す．

$$714 = \underset{\text{商}}{\underline{2}} \times 252 + \underset{\text{余り}}{\underline{210}}. \tag{2.4}$$

このとき，上と同様に考えて，$\gcd(714, 252) = \gcd(252, 210)$.

(Step 3) 元の問題は $\gcd(252, 210)$ を求める問題に変わったので，252 と 210 に対して，(Step1) を繰り返す．

$$252 = \underset{\text{商}}{\underline{1}} \times 210 + \underset{\text{余り}}{\underline{42}}. \tag{2.5}$$

このとき，上と同様に考えて，$\gcd(252, 210) = \gcd(210, 42)$.

(Step 4) 元の問題は $\gcd(210, 42)$ を求める問題に変わったので，210 と 42 に対して，(Step1) を繰り返す．

$$210 = \underset{\text{商}}{\underline{5}} \times 42 + \underset{\text{余り}}{\underline{0}}. \tag{2.6}$$

ここで，割り切れたので，$\gcd(210, 42) = 42$ である．($\gcd(210, 42) = \gcd(42, 0) = 42$ と考えても良い．) 以上より，$\gcd(2394, 714) = 42$.

この方法は，考える整数がどんどん小さくなっていくので，どんな 2 つの数から始めても必ずいつか割り切れて終わるということが容易に想像できるだろう．(厳密な取り扱いについては，補足プリント「拡張ユークリッド互除法について」を参考にすること．) これがユークリッド互除法である．

さて，ユークリッド互除法の各 Step を覚えておくことで，次のような問題に答えることができる．

問題

$2394x + 714y = 42$ を満たす整数の組 (x, y) を 1 つ求めよ．

解. ユークリッド互除法での計算を “逆にたどる”.

$$\begin{aligned}
42 &= 252 - 1 \times 210 \quad (\text{(2.5) より}) \\
&= 252 - 1 \times (714 - 2 \times 252) \quad (\text{(2.4) より}) \\
&= (-1) \times 714 + 3 \times 252 \\
&= (-1) \times 714 + 3 \times (2394 - 3 \times 714) \quad (\text{(2.3) より}) \\
&= 3 \times 2394 + (-10) \times 714
\end{aligned}$$

これより，$2394x + 714y = 42$ を満たす整数の組 (x, y) の例として，$(x, y) = (3, -10)$ が取れる． □

この解で行ったような，ユークリッド互除法を逆にたどるアルゴリズムを**拡張ユークリッド互除法**と呼ぶ．なお，$2394x + 714y = 42$ を満たす整数の組 (x, y) を 1 つ見つければ，全ての整数解も次のように求められる．つまり，以下の問題に答えることができる．

問題

$2394x + 714y = 42$ を満たす整数の組 (x, y) を全て求めよ．

解. $2394x + 714y = 42$ を満たす整数の組 (x, y) の 1 つとして，$(x, y) = (3, -10)$ が存在する (拡張ユークリッド互除法で見つける)．これより，

$$\begin{aligned}
&2394x + 714y = 42 \\
&\Leftrightarrow 2394(x - 3) + 714(y - (-10)) = 0 \\
&\Leftrightarrow 57(x - 3) + 17(y + 10) = 0 \quad (\text{両辺を } 42 = \gcd(2394, 714) \text{ で割る．})
\end{aligned}$$

最大公約数で割ったので，57 と 17 は互いに素であることに注意すると，最後の等式が成立するためには，

$$(x - 3, y + 10) = (17m, -57m),\ m \in \mathbb{Z}$$

という形であることが必要十分である．よって，$2394x + 714y = 42$ を満たす整数の組 (x, y) は

$$(x, y) = (3 + 17m, -10 - 57m),\ m \in \mathbb{Z}$$

が全てである． □

以上の手法を一般的な言葉を使ってまとめておこう．

正の整数 a, b, 整数 k に対して，

$$ax + by = k \gcd(a, b)$$

を満たす整数の組 (x, y) は次のようにして全て求められる．

(Step 1) ユークリッド互除法で $\gcd(a, b)$ を求める．この際，途中計算を記録しておく．

(Step 2) ユークリッド互除法の計算を逆にたどる拡張ユークリッド互除法を用いて $ax + by = \gcd(a, b)$ を満たす整数の組 (x'_0, y'_0) を 1 つ求める．

(Step 3) $x_0 \coloneqq kx'_0, y_0 \coloneqq ky'_0$ とすれば，(x_0, y_0) は $ax_0 + by_0 = k \gcd(a, b)$ を満たす整数の組である．

(Step 4) $a' \coloneqq a/\gcd(a, b), b' \coloneqq b/\gcd(a, b)$ とすると，a' と b' は互いに素で，

$$ax + by = k \gcd(a, b) \Leftrightarrow a'(x - x_0) + b'(y - y_0) = 0$$

であるので，これを満たすためには，

$$(x - x_0, y - y_0) = (b'm, -a'm),\ m \in \mathbb{Z}$$

が必要十分である．

(Step 5) $ax + by = k \gcd(a, b)$ を満たす整数の組 (x, y) は

$$(x, y) = (x_0 + b'm, y_0 - a'm),\ m \in \mathbb{Z}$$

が全てである．

また，以下の定理も重要である．

定理 2.4

正の整数 a, b に対して，以下の (1) と (2) は同値である：

(1) $ax + by = d$ を満たす整数の組 (x, y) が存在する．
(2) $[d]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$．

証明． (1) $\Rightarrow$ (2)：a, b は $\gcd(a, b)$ の倍数なので，$ax_0 + by_0 = d$ を満たす整数の組 (x_0, y_0) が存在するとき，

$$[d]_{\gcd(a,b)} = [ax_0 + by_0]_{\gcd(a,b)} = [0]_{\gcd(a,b)}.$$

(2) $\Rightarrow$ (1)：$[d]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$ のとき，ある $k \in \mathbb{Z}$ を用いて，$d = k\gcd(a, b)$ と書ける．$ax + by = k\gcd(a, b)$ を満たす整数の組 (x, y) が存在することは上でまとめた通りである． □

系 2.5

正の整数 a, b に対して，以下の (1) と (2) は同値である：

(1) $ax + by = 1$ を満たす整数の組 (x, y) が存在する．
(2) a と b は互いに素．(つまり，$\gcd(a, b) = 1$．)

証明． $[1]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$ が成立するのは $\gcd(a, b) = 1$ のときのみなので，定理 2.4 より主張は成立する．
□